ABSTRACT

Finite field multiplication of first and second Galois elements having n bit places and belonging to a Galois field GF 2^n described by an irreducible polynomial is performed by forming an intermediate result Z of intermediate sums of partial products of bit width 2n -2 in an addition part of a Galois multiplier. The intermediate result Z is processed in a reduction part of a Galois multiplier by modulo dividing by the irreducible polynomial, whereby after all XOR's are traversed a result E with n bits is computed.